ISTRUZIONE OPERATIVA _____

LISTA AGGIORNAMENTI

Revisione	Data	Descrizione delle modifiche apportate
1		Nuova codifica documento (ex I.) e aggiornamento processo e responsabilità

Autori del Documento	Funzione	Nome
Redatto da		
Verificato da		
Approvato da		

SOMMARIO:

1 - SCOPO

La presente istruzione definisce e regola le attività messe in atto da *[Associazione Nazionale Centri Sociali, Comitati Anziani e Orti – Coordinamento [●] ("Ancescao") / centro sociale [●] affiliato Ancescao ("Centro Sociale")]* al fine di garantire il corretto espletamento normativo nella raccolta dei dati e segnalazione al Garante in caso si verifichi e venga scoperto un *data breach* che coinvolga dati personali o sensibili/appartenenti a categorie particolari.
Essa è stata elaborata allo scopo di:
- rispondere pienamente alla normativa vigente in materia di privacy;
- operare nel continuo miglioramento degli strumenti di protezione dei dati personali;

2 - CAMPO DI APPLICAZIONE

La presente procedura si applica alle attività di gestione dei sistemi informativi operate dagli amministratori di sistema nel trattamento di dati personali e/o sensibili/ appartenenti a categorie particolari residenti nelle strutture informative di *[Ancescao/Centro Sociale]*

3 - TERMINOLOGIA E DEFINIZIONI

Per *data breach* si intende una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

4 - RESPONSABILITÁ

Le funzioni coinvolte nell'attuazione della presente procedura sono riportate nel quadro seguente:

FUNZIONE	RESPONSABILITA'
IT	- Operare quotidianamente applicando le misure di sicurezza adeguate all'attenuare per quanto possibile il verificarsi di *data breach*. - Identificazione del *data breach*. - Raccolta delle informazioni al fine di valutare con la direzione la necessità della segnalazione al Garante. - Salvataggio delle informazioni necessarie a tracciare il *data breach*.
Direzione/Presidenza/legale rappresentante	- Notificazione al Garante dell'avvenuto *data breach*. - Collaborazione con IT nell'attuare le opportune misure di tutela dei dati a livello organizzativo
Dipendenti/volontari	- Segnalazione agli amministratori di sistema di *data breach* di cui si viene a conoscenza.

5 - MODALITÁ ATTUATIVE

Quando, tramite segnalazione o per scoperta nelle proprie attività quotidiane, gli amministratori di sistema vengono a conoscenza di un avvenuto *data breach* devono attenersi alla seguente procedura:

1. Apertura di un *ticket* con categoria "*Incident* sicurezza" descrivendo nei dettagli i dati coinvolti nel *data breach* e le informazioni che hanno portato all'identificazione dello stesso. Inoltre, sul ticket è necessario censire:
    a. gli apparati coinvolti;

   b. la data ed ora ed il luogo dell'evento;
   c. il numero approssimativo di persone i cui dati personali sono stati coinvolti dal *data breach*;
   d. le tipologie di dati coinvolti;
   e. le misure tecniche ed organizzative di sicurezza presenti sui dati.
2. Il personale IT, se tecnicamente possibile, estrae e salva i log degli apparati coinvolti, inserendoli in contenitori non modificabili (come archivi RAR bloccati da MD5) per future analisi. Questi dati devono essere allegati al *ticket* precedentemente creato.
3. Una volta generato il *ticket*, lo stesso viene preso in carico dal personale IT.
4. Il personale IT incaricato di processare il *ticket* che ha come oggetto il *data breach* informa del fatto il responsabile IT, il legale rappresentante ed il comitato di direzione/presidenza/legale rappresentante.
5. La direzione/presidenza/legale rappresentante, di concerto con il personale IT ed il consulente Privacy decide se:
   a. È necessario effettuare comunicazione al Garante dell'avvenuto *data breach*. In caso si decida di non effettuare comunicazione al Garante allora la decisione sarà riportata sul *ticket* e si procederà direttamente all'esecuzione del punto 8.
   b. È ritenuto opportuno effettuare comunicazione agli interessati del *data breach* e l'eventuale modalità scelta. In ogni caso la decisione presa andrà motivata sul *ticket* e l'eventuale attività di invio dovrà essere opportunamente rendicontata al fine della compilazione del modulo di comunicazione al Garante di cui al punto 6.
6. Gli amministratori di sistema compileranno il modulo di segnalazione del *data breach* allegato alla presente procedura avendo cura di completare e dettagliare ogni sua parte, utilizzando i dati raccolti nel *ticket*.
7. Il legale rappresentante o l'eventuale delegato di *[Ancescao/Centro Sociale]*con potere di firma invierà la segnalazione al Garante dopo aver opportunamente firmato digitalmente il modulo.
8. Gli amministratori di sistema e la direzione/presidenza/legale rappresentante (o un delegato della stessa) analizzeranno i dati raccolti dall'analisi del *data breach* e decideranno le opportune misure di tutela dei dati sottratti e azioni organizzative e tecniche atte ad impedire futuri *data breach* della stessa natura. Tali decisioni dovranno essere riportate sul *ticket* di cui al punto 1. Al termine della segnalazione al Garante ciascuna di queste decisioni che richiedano un intervento da parte del responsabile IT dovranno essere riportate in appositi *ticket* per essere evase dal responsabile IT e relativi eventuali assistenti.

Per rispettare la normativa vigente le attività sopra descritte devono avere una durata massima di 72 ore, salvo ritardi giustificati ed opportunamente documentati, dalla scoperta del *data breach*.

Le attività e le verifiche eventualmente richieste dal Garante a seguito dell'invio del modulo di segnalazione *data breach* saranno valutate dalla direzione/presidenza/legale rappresentante. Le attività conseguenti di competenza del responsabile IT saranno opportunamente rendicontate e dettagliate nel *ticket* di cui al punto 1.

Le operazioni descritte nella presente procedura che coinvolgono la direzione/presidenza/legale rappresentante dovranno fare capo al legale rappresentante, in caso di assenza dello stesso un rappresentante del comitato di direzione/presidenza, con opportune deleghe, potrà farne le veci.

6 - INFORMAZIONI DOCUMENTATE

Nome Informazione Documentata	Responsabile Gestione	Luogo Archiviazione	Modalità della conservazione	Durata della conservazione